

**Apparatus for implementing a block encryption algorithm using round  
r petition**

Patent Number: EP1109350  
Publication date: 2001-06-20  
Inventor(s): CHABANNE HERVE (FR); TISSOT NICOLAS (FR)  
Applicant(s): SAGEM (FR)  
Requested Patent: ☐ EP1109350  
Application Number: EP20000403523 20001214  
Priority Number(s): FR19990015845 19991215  
IPC Classification: H04L9/06  
EC Classification: H04L9/06C  
Equivalents: ☐ FR2802741  
Cited Documents: NL1011800C; EP0981223

---

**Abstract**

---

The cypher algorithm technique has a digital word input (10) with two paths with input gates (12,14). A master key and sub keys are generated and injected by linear operations. Masks (M1,M2) are applied by the input of linear operations with the substitution of tables providing linear modifications.

---

Data supplied from the esp@cenet database - I2



(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 109 350 A1

(12)

## DEMANDE DE BREVET EUROPEEN

(43) Date de publication:

20.06.2001 Bulletin 2001/25

(51) Int Cl.7: H04L 9/06

(21) Numéro de dépôt: 00403523.4

(22) Date de dépôt: 14.12.2000

(84) Etats contractants désignés:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE TR

Etats d'extension désignés:

AL LT LV MK RO SI

(30) Priorité: 15.12.1999 FR 9915845

(71) Demandeur: SAGEM SA

75016 Paris (FR)

(72) Inventeurs:

• Chabanne, Hervé  
78200 Mantes-la-Jolie (FR)• Tissot, Nicolas  
95240 Corneilles-en-Parisis (FR)

(74) Mandataire: Fort, Jacques

CABINET PLASSERAUD

84, rue d'Amsterdam

75440 Paris Cedex 09 (FR)

(54) Dispositif mettant en oeuvre un algorithme de chiffage par bloc à répétition de rondes

(57) Le dispositif met en oeuvre un algorithme de chiffage par bloc à répétition de rondes comportant chacune des transformations linéaires, et des transformations non linéaires correspondant à des tables de substitution, utilisant une clé maître à partir de laquelle sont générées une ou des sous clés qui sont injectées dans les rondes par des opérations linéaires. L'algorithme applique des masques aux opérandes d'entrée par des opérations linéaires et en ce que les tables de substitution sont prévues pour qu'une modification linéaire de leur entrée provoque une modification linéaire de leur sortie.

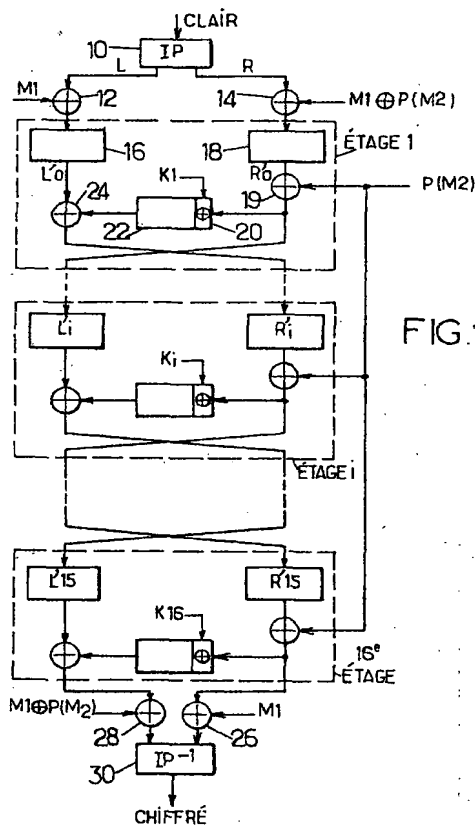


FIG.1.

## Description

[0001] La présente invention concerne les dispositifs mettant en oeuvre un algorithme de chiffage fournissant, à partir d'une donnée d'entrée en clair de longueur déterminée, un cryptogramme ou donnée de sortie qui dépend de la donnée d'entrée et d'une clé mémorisée inaccessible en lecture depuis l'extérieur du dispositif.

[0002] L'invention est applicable aux dispositifs du genre mettant en oeuvre un chiffage par bloc à répétition de rondes comportant chacune :

- des transformations linéaires et
- des transformations non linéaires correspondant à des tables de substitution et utilisant une clé maître à partir de laquelle sont générées une ou des sous clés qui sont injectées dans les rondes grâce à des opérations linéaires.

[0003] Elle trouve un intérêt particulier dans les dispositifs de chiffage mettant en oeuvre l'algorithme DES (data encryption standard) dont une description pourra être trouvée dans "Cryptographie Appliquée" par Bruce Schneier, traduction française, 2<sup>ème</sup> Edition, International Thomson Publishing, pages 281 et suivantes. Cet algorithme est à l'heure actuelle utilisé dans les cartes à puce pour fournir, à partir d'une donnée d'entrée en clair de 8 octets et d'une clé maître de 56 éléments binaires ou bits utiles, un cryptogramme ou donnée de sortie.

[0004] Un dispositif mettant en oeuvre l'algorithme de chiffage DES peut être regardé comme ayant 16 étages en cascade, chaque étage recevant une entrée de 2 x 32 bits. L'étage d'entrée est précédé d'un permutateur d'entrée fournissant 32 bits constituant une partie gauche et 32 bits constituant une partie droite, les 32 bits constituant des opérands. Le dernier étage est suivi d'un permutateur effectuant l'opération duale.

[0005] Chaque étage comporte :

- un élément d'expansion augmentant la taille de la partie droite, et
- un ensemble ou "ronde" ayant en cascade un opérateur OU EXCLUSIF ou XOR sur l'opérande droit expansé et une sous-clé de même longueur dérivée de la clé maître et des tables de substitution ou "S-boxes" affectées chacune à un groupe de bits et à lecture dans un ordre arbitraire et un opérateur XOR sur le contenu lu dans les tables et l'opérande gauche expansé pour donner naissance à une partie gauche de 32 bits constituant une des sorties de l'étage, l'autre sortie étant constituée par le résultat de la première opération XOR.

[0006] L'algorithme DES, tel qu'il est mis en oeuvre dans les cartes à puce, opère de la façon suivante. La donnée d'entrée est transformée en 16 étages successifs, à chacun desquels est affectée une sous-clé de 8 x 6 bits et on découpe chaque opérande, dans l'état où il est fourni à l'étage, en 8 tables de chacune 6 octets utiles.

[0007] Les algorithmes définis, et notamment l'algorithme DES sont attaquables par analyse différentielle de consommation de courant, du fait qu'ils sont en règle générale mis en oeuvre avec des circuits C-MOS qui ne consomment du courant que lors des changements d'état. Ce mode d'attaque de l'algorithme DES est décrit dans l'article de Chari et al. "Towards Sound Approaches to Counteract Power Analysis Attacks", Acte de la Conférence Crypto 99. Il repose sur des tests systématiques sur toutes les sous-clés possibles. On calcule des bits ayant participé au calcul à partir de chaque sous-clé choisie. Les mesures de consommation sont ensuite réparties en deux ensembles qui font apparaître un biais si la sous-clé est correcte. On remonte ainsi les étages ou itérations de l'algorithme. Dans le cas du DES mis en oeuvre sur les cartes à puce, à 16 étages et avec une clé de 64 bits (dont 56 bits utiles), donnant naissance à 16 sous-clés de 48 bits affectées chacune à une table, elles-mêmes scindées en 8 sous-clés élémentaires de 6 bits, un millier d'accès à la carte permet de déterminer la clé.

[0008] Le procédé pour rendre l'algorithme DES plus robuste qui est proposé dans l'article mentionné plus haut utilise la constatation que l'on peut interdire ou au moins gêner l'analyse différentielle de consommation, souvent appelée DPA, en manipulant les données de façon que les bits que l'attaquant calcule à partir de sa connaissance de l'algorithme et des entrées/sorties de la carte soit sans rapport avec les opérations réalisées dans la carte.

[0009] Pour cela, l'article propose d'appliquer un masque aléatoire aux sous-clés K intervenant à chaque étage i ou à certains des étages. Mais cette solution présente l'inconvénient de compliquer énormément les calculs, car le masque ne se conserve pas dans les étages successifs.

[0010] Un but général de l'invention est d'augmenter la résistance à l'attaque, par analyse différentielle de consommation, des algorithmes du genre défini ci-dessus. Dans ce but elle propose un dispositif suivant la revendication 1.

[0011] L'idée de base est de faire en sorte que les bits que l'attaquant calcule à partir de sa connaissance de l'algorithme et des entrées/sorties de la carte n'aient aucun rapport avec la réalité des opérations réalisées par la carte. Cela revient en fait à "masquer" les opérations en appliquant, via un "OU EXCLUSIF", un masque aléatoire à chacun des opérands (et non pas des sous-clés) afin que les bits intervenant dans les calculs n'aient, a priori, qu'une chance sur deux d'être les mêmes qu'auparavant.

[0012] La présente invention vise surtout à fournir un dispositif mettant en oeuvre un algorithme de chiffage four-

## EP 1 109 350 A1

nissant les mêmes résultats que les algorithmes ci-dessus DES (ou autres, tels que AES et Kasami), mais assurant une résistance très élevée à l'attaque par analyse différentielle de consommation, sans complication excessive des calculs.

[0013] Il est en conséquence proposé, suivant un autre aspect de l'invention, un dispositif de chiffrement mettant en oeuvre un algorithme donnant la même sortie que l'algorithme DES, suivant la revendication 2.

[0014] Les termes "gauche" et "droit" ne sont utilisés que par commodité et sans que cela ait un sens quant à une disposition des opérandes. Les opérations successives peuvent être faites par voie logicielle ou matérielle.

[0015] La constitution ci-dessus exploite le fait que les opérations OU, les opérations OU exclusif XOR, les expansions E et les permutations P ont un caractère linéaire, c'est-à-dire que, si on appelle M un octet d'un masque et A et B ceux de deux opérandes, on a :

$$A \oplus (B \oplus M) = (A \oplus B) \oplus M$$

$$E(A \oplus M) = E(A) \oplus E(M)$$

$$P(A \oplus M) = P(A) \oplus P(M)$$

[0016] Seul le passage dans les tables, dites "S BOX", n'est pas linéaire, ce qui oblige à constituer les tables de façon différente de celle utilisée pour mettre en oeuvre l'algorithme DES classique.

[0017] Si on désigne par S l'opération effectuée par les tables d'un étage et par A et B les opérandes, l'opération :

$$S(E[A]) = B$$

est à remplacer par :

$$S(E[A] \oplus M_1) = B \oplus M_2 = S(E[A]) \oplus M_2$$

mettant en oeuvre des opérations OU EXCLUSIF.

[0018]  $M_1$  ou  $M_2$  désignent des masques tirés aléatoirement.

[0019] On verra que la modification qui en résulte sur le schéma habituel du DES est simple : on masque L et R, après avoir réalisé la permutation initiale IP, avec respectivement  $M_1$  et  $M_1 \oplus P(M_2)$ . Par ailleurs, avant chaque entrée dans une ronde, on réalise un OU EXCLUSIF entre R et  $P(M_2)$ .

[0020] Comme on le verra plus loin, les masques se conservent après passage dans les boîtes et cette propriété permet de répéter sans calcul supplémentaire la protection sur tous les ensembles successifs et donc d'obtenir une protection maximale sans complication additionnelle. On voit donc l'intérêt de l'application d'un masque aux opérandes, comparée à l'application d'un masque aux sous-clés.

[0021] L'invention n'est pas applicable seulement à l'algorithme DES, mais également à tout autre algorithme de chiffrement mettant en oeuvre surtout des opérations de nature linéaire et des opérations dans lesquelles il y a conservation du masque sur les étages successifs.

[0022] Les caractéristiques ci-dessus, ainsi que d'autres, apparaîtront mieux à la lecture de la description qui suit de la mise en oeuvre de l'invention dans un dispositif de chiffrement dérivé de dispositifs couramment utilisés dans les cartes à puce, ayant  $2n = 16$  étages ou itérations.

[0023] La description se réfère aux figures qui l'accompagnent dans lesquelles :

- la figure 1 est un schéma du dispositif,
- la figure 2 est un schéma d'un étage.

[0024] Le dispositif représenté comporte 16 étages de constitution identique. Les données d'entrée en clair, qu'on supposera par la suite être constituées, soit de 8 octets, soit 64 bits sont appliquées à un permuteur d'entrée 10, qui effectue une permutation IP. Ce permuteur fournit en sortie une partie gauche L de 32 bits et une partie droite R également de 32 bits. Avant d'entrer dans les étages successifs 1, ..., 16, les parties L et R, qui constituent des opérandes, sont soumises à des opérations logiques XOR au niveau du bit, dans des portes 12 et 14 :

$$L \oplus M_1$$

$$R \oplus M_1 \oplus P(M_2)$$

[0025]  $M_1$  et  $M_2$  sont des masques de 32 bits qui seront utilisés dans chaque étage du dispositif, mais sont aléatoires, c'est-à-dire changent à chaque accès au dispositif, on obtient ainsi en 16 et 18 des opérandes  $L'_0$  et  $R'_0$  pour le premier étage.

[0026] Dans chaque étage, la partie droite qui résulte de l'opération XOR en 14 est soumise à expansion E portant sa longueur de 32 à 48 bits, comme indiqué en 18 pour l'étage: 1. La partie droite  $R'_0$  est soumise en 19 à une opération XOR avec  $P(M_2)$  qui compense l'opération faite en 14. La partie droite ainsi modifiée, comportant 48 bits, est combinée en 20 avec une sous-clé de 48 bits par une opération XOR. Chacune des sous-clés  $K_1, \dots, K_{16}$  est constituée à partir de la clé maître par décalage et sélection de 48 bits parmi les 56 bits de la clé maître. Cette opération XOR 20 constitue le premier élément d'une ronde ou "round", identique dans chaque étage et effectuée dans une table de substitution 22 par un algorithme de substitution mémorisé. La sortie de la ronde est combinée avec la moitié gauche  $L'_0$  (pour l'étage 1) par une nouvelle opération XOR 24 et les sorties sont croisées de sorte que la moitié gauche devient la moitié droite et inversement.

[0027] A l'issue de la ronde du dernier étage, la partie droite est combinée au masque  $M_1$  par une opération XOR 26 tandis que la partie gauche est combinée avec le résultat de l'opération  $M_1 \oplus P(M_2)$  par une opération XOR 28. Enfin le résultat est soumis en 30 à une permutation  $IP^{-1}$  inverse de la permutation initiale.

[0028] Une comparaison entre les résultats intermédiaires obtenus par l'algorithme DES classique et par l'algorithme modifié conformément à l'invention fait apparaître les différences.

[0029] Si on désigne par  $L_i$  et  $R_i$  les parties gauche et droite de la  $i$ ème itération ( $i$ ème étage) de l'algorithme DES standard et par  $L'_i$  et  $R'_i$  les parties gauche et droite du DES modifié conformément à l'invention, on a :

$$R'_i = R_i \oplus M_1 \oplus P(M_2)$$

$$L'_i = L_i \oplus M_1$$

[0030] L'opération XOR avec  $P(M_2)$  avant expansion implique :

$$S(E[R'_i \oplus P(M_2) \oplus K] \oplus M_1)) = S(E[R_i \oplus K]) \oplus M_2$$

et comme  $L_{i+1} = R_i$  et  $R_{i+1} = P(S(E[R_i \oplus K])) \oplus L_i$  il vient :

$$L_{i+1}' = R'_i \oplus P(M_2) = R_i \oplus M_1$$

ce qui donne  $L_{i+1}' = L_{i+1} \oplus M_1$ , et

$$R_{i+1}' = P(S(E[R_i \oplus K] \oplus M_2) \oplus L_i) = P(S(E[R_i \oplus K])) \oplus P(M_2) \oplus L_i \oplus M_1$$

ce qui donne  $R_{i+1}' = R_{i+1} \oplus M_1 \oplus P(M_2)$

[0031] Ces formules font apparaître que les masques  $M_1$  et  $M_2$  se conservent au passages dans les tables successives.

[0032] Les opérations XOR finales en 26 et 28 (démasquage de  $L_{16}$  et  $R_{16}$  juste avant la permutation finale) et conduisent au même résultat que le DES standard.

[0033] L'avantage de l'invention découle de l'incertitude qu'elle provoque en cours de calcul sur les bits et qui découle du masquage. Il y a une possibilité de  $\frac{1}{2}$  pour qu'un chaque bit soit transformé en son complémentaire par l'opération de masquage. Comme les masques changent à chaque nouvel appel au DES, il est impossible de déterminer quels sont les bits masqués et quels sont ceux qui ne le sont pas. Par conséquent l'attaquant ne peut plus distinguer, même lorsqu'il a deviné et essayé la bonne sous-clé, les valeurs des bits. L'attaque par DPA n'est plus possible. Expérimentalement aucun biais n'est apparu sur 10.000 accès au DES. L'accroissement de complexité requis est raisonnable.

## EP 1 109 350 A1

Dans la mise en oeuvre sur les carte à puce (16 étages et données de 64-bits), le recalcul dans les tables des rondes et le recalcul systématique n'exigent qu'à 256 octets en mémoire vive. Le temps d'exécution du DES passe de 12 à 25 ms. Mais l'algorithme est englobé dans un processus nécessitant la récupération de la commande de chiffrement et des paramètres, de sorte que la perte de temps n'est que de l'ordre de 18 %. On passe de 72 à 85 ms et le code assembleur passe de 1000 à 1300 octets, ce qui est très tolérable au vu du résultat obtenu.

### Revendications

1. Dispositif mettant en oeuvre un algorithme de chiffrement par bloc à répétition de rondes, chaque ronde comportant :

des transformations linéaires, et  
des transformations non linéaires

consistant à faire passer des données à travers des tables ou boîtes de substitution, utilisant une clé-maître à partir de laquelle sont générées une ou des sous-clés qui sont injectées dans les rondes par des opérations linéaires,

caractérisé en ce qu'il applique des masques aux opérandes d'entrée par des opérations linéaires et en ce que les tables de substitution sont prévues pour qu'une modification linéaire de leur entrée provoque une modification linéaire de leur sortie.

2. Dispositif mettant en oeuvre un algorithme de chiffrement donnant la même sortie que l'algorithme DES, comportant :

- un permuteur initial P partageant l'entrée en une partie gauche L et une partie droite R chacune de 32 bits,
- un opérateur d'entrée XOR entre la partie gauche L et un masque aléatoire  $M_1$  de même longueur,
- un opérateur d'entrée XOR entre la partie droite R et le résultat de l'opération XOR effectuée sur  $M_1$  et sur une permutation P d'un masque aléatoire  $M_2$ ,
- 16 étages en cascade, chaque étage recevant une entrée de  $2 \times 32$  bits de l'étage précédent et ayant :
  - un élément d'expansion de la partie droite masquée, donnant naissance à une valeur expansée  $R'_1$ ,
  - une porte XOR de compensation, effectuant l'opération XOR sur  $R'_1$  et la permutation P( $M_2$ ),
  - une ronde effectuant l'opération XOR entre la sortie de la porte de compensation XOR et la valeur  $L_1$ , et ayant des tables de substitution affectées chacune à un groupe de bits, à lecture dans un ordre arbitraire et un opérateur XOR sur le contenu lu dans les tables et la partie gauche pour donner naissance à une partie gauche de sortie de 32 bits, l'autre sortie étant constituée par la sortie de la porte de compensation, l'opération effectuée par les tables d'un étage sur des opérandes d'entrée A et B étant de la forme :

$$S(E[A] \oplus M_1) = B \oplus M_2 = S(E[A]) \oplus M_2$$

et les parties gauche et droite  $L'_1$  et  $R'_1$  du ième étage étant reliées aux parties gauche et droite  $L_i$  et  $R_i$  de l'algorithme DES standard par les relations :

$$R'_1 = R_1 \oplus M_1 \oplus P(M_2)$$

$$L'_1 = L_1 \oplus M_1$$

- des opérateurs XOR de démasquage effectuant, en aval du dernier étage, les mêmes opérations qu'en entrée,
- un permuteur effectuant l'opération  $P^{-1}$  duale de la permutation P d'entrée.

3. Dispositif selon la revendication 1, caractérisé en ce que les opérations (S) effectuées dans les tables de substitution sont de la forme :

$$S(E[A] \oplus M_1) = B \oplus M_2 = S(E[A]) \oplus M_2$$

## EP 1 109 350 A1

où :

$\oplus$  désigne l'opération ou EXCLUSIF bit à bit

E désigne une expansion

$M_1$  désigne un manque aléatoire appliqué sur une partie gauche d'entrée

$M_2$  désigne un masque aléatoire

A et B désignant les opérandes d'entrée



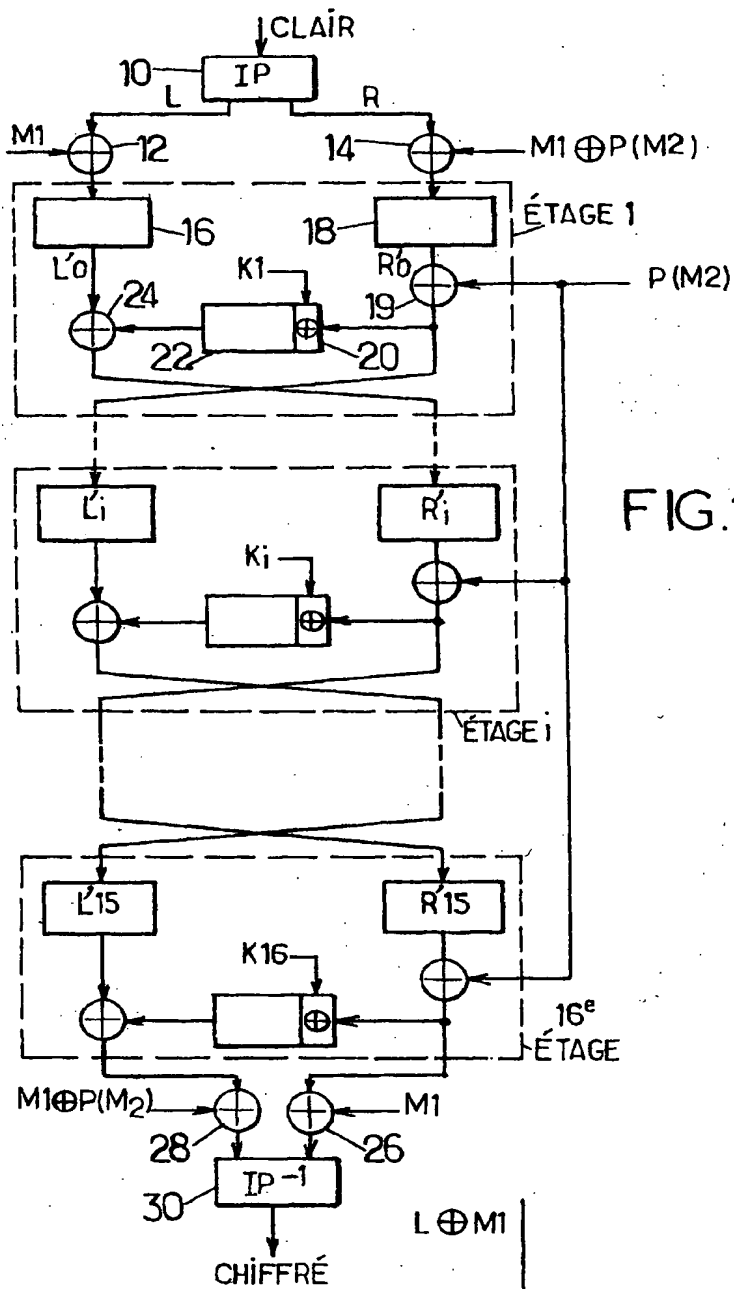
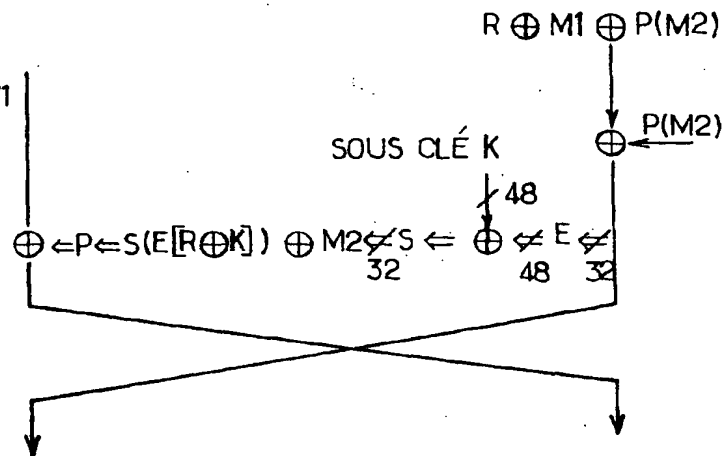


FIG. 2.





Office européen  
des brevets

# RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande  
EP 00 40 3523

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X	NL 1 011 800 C (KPN) 24 novembre 1999 (1999-11-24)	1	H04L9/06
A	* page 3, ligne 28 - page 4, ligne 3 *	2	
P, X	* page 11, ligne 15 - page 13, ligne 4 * -& WO 00 41356 A (KPN) 13 juillet 2000 (2000-07-13)	1	
P, X	* page 3, ligne 22 - ligne 37 * * page 11, ligne 1 - page 12, ligne 28 * EP 0 981 223 A (TOKYO SHIBAURA ELECTRIC CO) 23 février 2000 (2000-02-23) * abrégé; figures 11, 14 * * colonne 12, ligne 18 - colonne 13, ligne 38 * * colonne 14, ligne 16 - colonne 15, ligne 31 *	1	
Le présent rapport a été établi pour toutes les revendications			DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)
			H04L
Lieu de la recherche		Date d'achèvement de la recherche	Examineur
LA HAYE		26 mars 2001	Holper, G
CATEGORIE DES DOCUMENTS CITES			
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : entière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	

EPO FORM 1503 (03.92) (P04002)

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE  
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 00 40 3523

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.  
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du  
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

26-03-2001

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
NL 1011800 C	24-11-1999	NL 1010921 C	03-07-2000
		NL 1011544 C	03-07-2000
		AU 1983300 A	24-07-2000
		WO 0041356 A	13-07-2000
		NL 1011800 A	03-06-1999
EP 0981223 A	23-02-2000	JP 2000066585 A	03-03-2000

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

